(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
8 January 2004 (08.01.2004)

PCT

(10) International Publication Number
WO 2004/004199 A1

(51) International Patent Classification⁷: H04L 9/32, 9/08, H04Q 7/38

(21) International Application Number: PCT/EP2002/007076

(22) International Filing Date: 26 June 2002 (26.06.2002)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: TELEFONAKTIEBOLAGET LM ERICSSON (publ) [SE/SE]; S-126 25 Stockholm (SE).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: HOWARD, Joe [IE/IE]; 158 Brandon Road, Drimnagh, Dublin 12 (IE).

(74) Agents: HOFFMANN.EITLE et al.; Arabellastrasse 4, 81925 München (DE).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

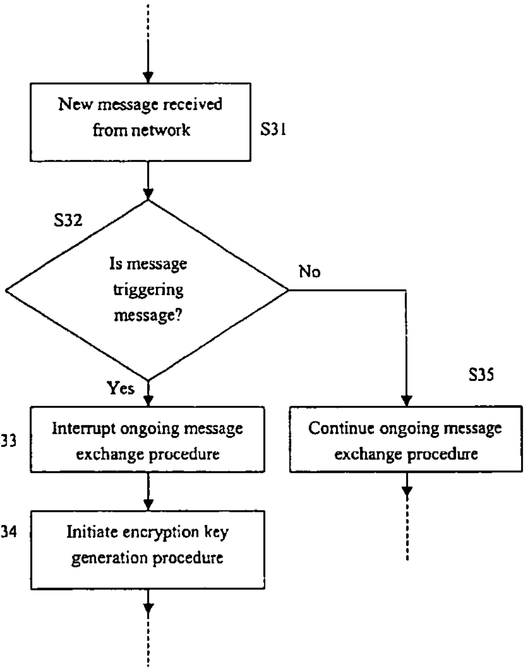
(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declaration under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW, ARIPO patent (GH, GM, KE, LS,*

[Continued on next page]

(54) Title: METHOD OF CONTROLLING A NETWORK ENTITY AND A MOBILE STATION


New message received from network
S31
S32
Is message triggering message?
No
Yes
S35
S33
Interrupt ongoing message exchange procedure
Continue ongoing message exchange procedure
S34
Initiate encryption key generation procedure

(57) Abstract: A method of controlling a network entity (4, 5) of a mobile communication network and a mobile station (1) is described, as well as a corresponding mobile station and network entity. The network entity (4, 5) and the mobile station (1) are arranged to conduct a plurality of predetermined message exchange procedures in the course of which predetermined messages are exchanged between said network entity (4, 5) and said mobile station (1) depending on the given procedure. The predetermined messages may be encrypted, an encrypted message being any message of which at least a part is encrypted. The network entity (4, 5) and the mobile station (1) are furthermore arranged to conduct one or more encryption key generation procedures in parallel during which the network entity (4, 5) and the mobile station (1) generate and store respective corresponding encryption keys, in order to be able to encrypt and decrypt exchanged messages. The method comprises a step of determining (S21) whether a received message from the mobile station is encrypted. If the received message is encrypted, it is determined (S22) whether a correct encryption key for decrypting said message is available to said network entity (4, 5), and if no correct key is available, a predetermined triggering message is sent to said mobile station (1). The mobile station (1) then interrupts (S33) the procedure in the course of which it sent the encrypted message for which the network entity (4, 5) did not have a correct key, and initiates (S34) an encryption key generation procedure.